December 2022 | Volume 2

MCI MicroBIT

MAGNOLIA CYBERSECURITY INSTITUTE NEWSLETTER

STUDENT LEADERSHIP SUMMIT

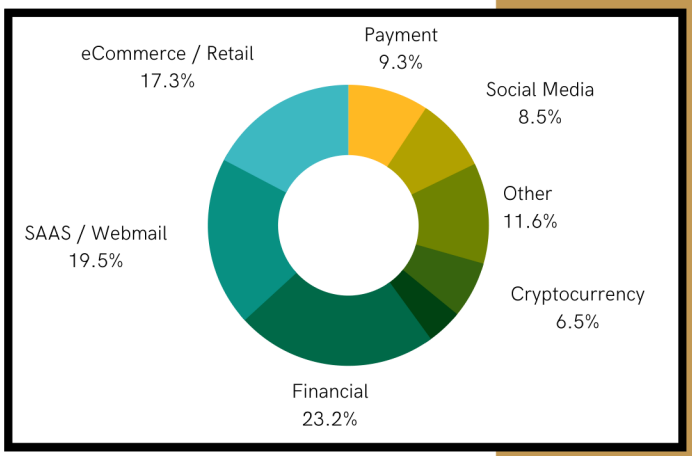
By Alyssa Muldong

On November 30, 2022, Vital Link hosted a county-wide event for all high school student leaders who wish to learn and expand their knowledge on becoming better leaders. Students had the opportunity to visit three different workshops that piqued their interest. Workshops that were offered ranged from learning to network with partnered company employees to boosting your entrepreneurial confidence to become a problem solver. Throughout the summit, high school students got to learn more about their peers at the event. Many opportunities were being offered to take initiative such as experiencing public speaking in front of a huge audience. The Summit allowed every student leader to explore the awesome opportunities that await them and become inspired to help inspire others to do the same.

Magnolia High School was invited to participate in this awe-inspiring event. 47 students were selected to represent Magnolia High. Each student got to discover opportunities that seemed like the best fit for them out of the total of 23 exhibitors including 13 colleges to browse through. Guest speakers gave out their unique speeches on how they got to the position they are in today, to think outside of the box, and to use their creativity. During the break, students received free lunch where students got to chat with other employees to start creating a network. To end off with the event, students got to go from table to table to chat with a partnered company employee to help speed mentor those that are interested. High school students from Magnolia High have enjoyed the event, greatly appreciated the invitation, and will take back something that they have learned.

CURRENT PHISHING ATTACKS

By Ashley and Ansley Sousa



Phishing is a social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware.

In the 12 months from July 2021 to June 2022, 55% of Comcast Business customers experienced botnet attacks, while nearly 50% had to contend with malware and phishing attacks. According to Internet activity, the researchers monitored, financial and high-tech brands were the most targeted by phishing scams at 41% and 36%, respectively.

Scammers use email or text messages to try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could get access to your email, bank, or other accounts. Or they could sell your information to other scammers. Scammers launch thousands of phishing attacks like these every day — and they're often successful.

CYBER highlights

55 new cyber applicants are entering the MCI Exclusive Pathway in 2023-2024

MCI Construction Update: building beams are now visible

Cyber Range is coming to MHS in January 2023

Cyber Teams are preparing for the Cyber Olympics

CyberPatriot Teams completed third round of competition

MCI
MAGNOLIA CYBERSECURITY INSTITUTE
UNLEASH INNOVATION
SECURE OUR FUTURE

CYBER SAFETY TIPS

By Jed Dye

Four Ways to Protect Yourself from Phishing

1. Protect your computer by using security software. Set the software to update automatically so it will deal with any new security threats.

2. Protect your cell phone by setting software to update automatically. These updates could give you critical protection against security threats.

3. Protect your accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. The extra credentials you need to log in to your account fall into three categories:
   - like a passcode, a PIN, or the answer to a security question.
   - like a one-time verification passcode you get by text, email, or from an authenticator app; or a security key
   - like a scan of your fingerprint, your retina, or your face

Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

4. Protect your data by backing it up. Back up the data on your computer to an external hard drive or in the cloud. Back up the data on your phone, too.

PYTHON PROGRAMMING TO 3D PRINTING

By Letica Alvarado-Franco

The Python to 3D print project was a two-part assignment, tying together our new Python programming knowledge and our prior 3D printing experience. We spent two weeks finding the code necessary to create a unique shape in Python. From there, we began reproducing the image in a 3D Print. We were encouraged to develop unique designs and, as such, our obstacles were specific to the images we were creating. Using a combination of both collaborative and independent thinking, we crafted an amazing collection of designs.

Of course, there were days where, after hours of failed attempts, we made little to no progress. And because of this, collaboration played an enormous role in the success of our projects. Though the problems our peers encountered were unique to their projects, hearing their perspectives also inspired possible solutions. Our assignment was undoubtedly independent, however, it also encouraged interpersonal communication and welcomed original ideas. This journey has provided us with the tools to become innovative members of the cyber workforce.

TERMINOLOGY

Deepfake

A piece of audio or video that has been altered and changed to make it seem authentic or credible.

Ethical Hacking

With the owner's permission, breaches the network to obtain sensitive information—completely legal. Typically, this technique is used to check for infrastructure weaknesses.

Spyware

A form of malware used by hackers to spy on you and your computer activities. If a mobile device such as a smartphone is infected with spyware, a hacker can read your text messages, redirect your phone calls, and even track down where you are physically located!

Trojan Horse

A misleading computer program that looks innocent, but allows the hacker into your system via a back door, allowing them to control your computer.

Worm

Malware that can reproduce itself for the purposes of spreading itself to other computers in the network.

Upcoming Events

Cyber Oylmpics

January 17 - 26, 2023

Dale JHS March to Magnolia HS

February 1, 2023